UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THEODORE RIDER, JESSE W. SMITH, and GILLES BOEVI, individually and on behalf of other similarly situated individuals, Plaintiffs, v. UPHOLD HQ INC., a South Carolina corporation, and JOHN DOES 1–10, individuals, Defendants.	Civil Action No. 1:22-cv-01602 **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

INTRODUCTION

> *"To uphold something is to hold it aloft, prevent it from falling or sinking, to maintain and affirm. Our new brand represents our commitment to consumer protections and true transparent financial services accountability. In a word, Uphold embodies our core values and is the best way we can describe our bold vision of providing accessible, equitable, free and fair financial services to everyone, everywhere – secure in the cloud, real-time on any device."*
>
> -Uphold.com, Oct. 14, 2015[1]

1. Despite its lofty statements, the cryptocurrency exchange Uphold HQ Inc. ("Uphold") failed to correctly implement essential security protections for its customers, resulting in thousands of customers losing all of their cryptocurrency savings—and often, all of their life savings. This complaint is brought on behalf of a putative class of victims of Uphold's flawed security practices, including retirees, active-duty military, unemployed consumers, disabled

[1] Exhibit A, Welcome to Uphold. The Internet of Money, Uphold.com (Oct. 14, 2015), available at https://blog.uphold.com/welcome-to-uphold-the-internet-of-money.

consumers, and thousands of other victims who put their trust in Uphold to protect their funds, only to have those funds stolen due to Uphold's failed promises.

2. Plaintiff Gilles Boevi exemplifies the experience of thousands of others in the putative class of victims. On August 1, 2021, Plaintiff Boevi received an email notification from Uphold, the cryptocurrency exchange where he purchased and stored Ripple ("XRP") and Dogecoin ("DOGE"), that someone had initiated a transaction affecting his XRP holdings. Boevi had never initiated such a transaction, and he could not log into his Uphold account because someone had disabled his two-factor authentication. At the time, the combined value of the XRP and DOGE in Boevi's account on Uphold.com was $26,176.21.

3. In a panic, Boevi immediately contacted Uphold's support team to notify them that an unauthorized user had gained access to his account. The time was 9:44 AM EST. In the support ticket, he frantically explained that he was receiving notices of unauthorized transactions posted to his account.

4. Despite Uphold acknowledging Boevi's messages, they did **not** freeze Boevi's account to prevent further transactions. Boevi knew that time was of the essence, but all he could do was stand by, helplessly refreshing his account, while he waited for customer service to respond to his pleas.

5. Two hours and eleven minutes after he first notified Uphold of the unauthorized transactions to his account, the unauthorized user successfully transferred all of Boevi's cryptocurrency out of his account. Boevi refreshed his account to see his balance at $0.00.

6. Eleven minutes later, the Uphold support team froze his account.

7. During the weeks that followed, at Boevi's request, the same support team claimed to conduct an internal investigation, in which it concluded it was in no way responsible for the

loss. "Even though we are sure our platform wasn't compromised in any way whatsoever, our customers' satisfaction is our most valuable asset at the end of the day," the customer service representative assured him.[2]

8. But there was something else the Uphold representative mentioned in the same email, something that caught Boevi's attention. Like most users, when Boevi first created an Uphold account, he enrolled in two-factor authentication, an industry standard security measure that makes it nearly impossible for an unauthorized user to access an account, because the user must have access to a physical device in the accountholder's possession in addition to the account's login credentials.[3]

9. This security measure is crucial, because in a world where cybercrime is rampant, financial service providers cannot protect user accounts with usernames and passwords alone. Two-factor authentication ensures that even when a user's email and password are compromised, the account remains secure.

10. Boevi had enabled two-factor authentication using an authentication app on his phone, which was still in his possession before, during, and after the theft of his funds. But the email from Uphold indicated that Boevi's two-factor authentication device had been changed by the unauthorized user. Thus, Uphold permitted Boevi's two-factor authentication to be changed by a third party without Boevi's permission, evidencing security practices that clearly fall below the standard of care as well as breach Uphold's promises to its customers.

11. Uphold offered Boevi no recourse. It suggested instead that he report the cybercrime—not to the FBI or any regulatory agency equipped to deal with such a brazen theft—

[2] Exhibit B, Email from Ramses to Gilles.

[3] Two-factor authentication is typically conducted with the use of a code sent via SMS to a user's mobile phone, to enter as part of authentication; alternatively, an authentication app on a user's mobile device, like Google Authenticator, may be used to generate a unique code to enter as part of authentication.

but to his local law enforcement agency. Uphold also invited Boevi to have his lawyer contact Uphold's fraud team. And then Uphold moved on.

12. Boevi lost over $25,000 worth of cryptocurrency in a single day, but what he did not realize at the time was that he was far from the only user affected.

13. A month later, Uphold's security problems remained, as reflected in the experience of Plaintiff Jesse Smith, who is on active duty with the U.S. Navy and stationed in North Carolina. He created his Uphold account in December 2020, and he set up two-factor authentication with an authenticator app at that time.

14. On October 5, 2021, Smith opened his Uphold mobile app to discover his account had a zero balance, despite the that fact that he should have had $12,000 in XRP in his account. Smith also noticed that someone using an IP address located in Turkey had converted all of his XRP to Tether, then to Ethereum, prior to transferring the funds to an unknown account at Binance, despite Plaintiff Smith never receiving any notifications from Uphold about any changes or transactions in his account.

15. In the Uphold app, Smith noticed that his email had also been changed to an Outlook email that he had never seen before. Smith immediately contacted Uphold by online chat, and Uphold instructed him to send an email to customer support, which he did. Uphold froze his account four hours later, despite the fact that his cryptocurrency had already been stolen.

16. Uphold denied all fault in the theft of Smith's $12,000 in cryptocurrency, without any explanation, and Uphold suggested that he file a report with his local police department.

17. Plaintiff Theodore Rider's experience was also similar to the experience of thousands of others in the putative class of victims. He created his Uphold account in February 2021, and later he set up two-factor authentication with his Google Authenticator app. He

deposited most of his life savings into his Uphold account.

18. On November 12, 2021, Rider checked the balance in his Uphold account, which had been over $22,000 just days before. However, when he launched the Uphold mobile app, he could not log in. He tried logging in multiple times, without success, and quickly discovered that his two-factor authentication had been reset without his permission.

19. Rider immediately contacted Uphold on Twitter, Reddit, Facebook, and Instagram, in addition to emailing Uphold customer support. Each time, he informed Uphold that his account may have been compromised and requested that Uphold stop all transactions in the account. He did not hear back from Uphold, and Uphold did not freeze his account until the following week.The week after that, Uphold finally let him into his account, at which time he discovered that his Uphold account had a zero balance.

20. While Rider was waiting for Uphold to respond to his emails and other communications, all of his cryptocurrency was transferred out of his account. In addition, someone had initiated ACH transactions from within Rider's Uphold account, completely depleting his bank account and causing an overdraft of $2,500.

21. When Uphold finally responded to him, Uphold stated that someone had changed his email of record in his Uphold account, and thereafter changed his password, and thereafter changed his two-factor authentication device, despite the fact that he was never notified of any of these changes.

22. Uphold denied all responsibility for the theft and suggested that Rider file a report with his local police department.

23. Although Uphold never notified its customers of a data breach of any kind, the problem has quietly continued.

24. In the following months, many other Uphold customers continued to be victimized due to Uphold's faulty two-factor authentication processes, perhaps even thousands of customers. In fact, an Uphold representative informed one customer, in writing, that at least "10%" of Uphold's customers had been affected by similar fraudulent activity resulting in the theft of customer funds.

25. As of October 15, 2020, Uphold had approximately 2 million users.[4]

JURISDICTION AND VENUE

26. Plaintiffs bring this class action lawsuit on behalf of themselves and all others similarly situated (collectively, "Class Members") against Uphold HQ Inc., a South Carolina company with its principal place of business in New York, and allege the following based upon personal knowledge as to their own acts and upon information and belief upon the investigation of counsel as to all other matters.

27. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §1332(d) because the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, and this is a class action in which at least one member of the putative class is a citizen of a state different than Uphold. The proposed class consists of more than one hundred persons. Further, the claims can be tried jointly because they involve common questions of law and fact that predominate over the individual issues, as outlined below.

28. This Court has personal jurisdiction over Uphold consistent with due process and C.P.L.R. §302 because Uphold does business in this District on a systematic and ongoing basis; holds or owns real and personal property within this District; derives substantial revenue from its contacts within this District; has consented to personal jurisdiction in this District in the agreement

[4] *See* https://www.veriff.com/case-studies/interview-with-uphold-cio.

between Uphold and Plaintiffs (*see* Exhibit C); has committed tortious acts within this District; and is headquartered or maintains offices within this District.

29. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because Uphold resides in this District, and a substantial part of the events or omissions giving rise to the claims occurred in this District through offices maintained by Uphold in this District.

PARTIES

30. Plaintiff Theodore Rider is an individual, who at all times relevant to this action was a resident of the state of Michigan.

31. Plaintiff Gilles Boevi is an individual, who at all times relevant to this action was a resident of the state of New Jersey.

32. Plaintiff Jesse Smith is an individual, who at all times relevant to this action was a resident of the state of North Carolina.

33. Class Members are residents and citizens of different states who created accounts on Uphold.com and/or in the Uphold mobile application, and who subsequently had their Uphold accounts accessed by unauthorized cybercriminals.

34. Defendant Uphold is a South Carolina company with its principal place of business located at 530 5th Avenue, Suite 3A, New York, NY 10036.

35. Defendants John Doe 1–10 (the "Doe Defendants") are the individual founders, directors, officers, and agents of Defendant Uphold, whose identities are currently unknown to Plaintiffs, and who were responsible for developing and maintaining the integrity of Uphold's security systems, for ensuring Uphold's compliance with state and federal law, and for truthfully representing Uphold's characteristics and security protocols to Plaintiffs.

36. Uphold and the Doe Defendants, each of whom are the principals and agents and/or

alter egos of one another, acted on one another's behalf, and bear joint and several liability to Plaintiffs for their injuries.

37. Uphold purports to bind all its users, including Plaintiffs, to Terms and Conditions, a copy of which is attached hereto as **Exhibit C**. These Terms and Conditions dictate that New York law governs this dispute:

> 12.8 You agree that the laws of the State of New York, without regard to principles of conflict of laws, govern these Terms and Conditions and any claim or dispute between you and us except to the extent governed by U.S. federal law.

38. Defendant Uphold regularly engages in business throughout the State of New York, where it is headquartered and where it maintains its offices. The Doe Defendants likewise regularly engage in business in New York City and its contiguous counties and jurisdictions.

39. Whenever this Complaint refers to any act(s) of Defendants, Uphold, and/or the Doe Defendants, the reference shall be deemed to mean that the directors, officers, employees, affiliates, or agents of Defendants authorized such act while actively engaged in the management, direction, or control of the affairs of Defendants, and/or acts by persons who are the parents or alter egos of Defendants while acting within the scope of their agency, affiliation, or employment.

STATEMENT OF FACTS

Industry Background

40. Uphold is a cryptocurrency exchange that allows users to transfer, purchase, trade, hold, and sell various cryptocurrencies on its platform.

41. As with most financial technology ("FinTech") services, providers in the cryptocurrency industry are expected to guard against data breaches.

42. The Federal Trade Commission ("FTC") has issued numerous guides for businesses of all kinds, which highlight the importance of implementing reasonable protocols to ensure data security. In fact, the FTC cautions that this need for data security should be a factor in all business

decision making.[5]

43. In its 2016 publication, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, the FTC advised businesses to take measures to protect personal customer information. Some of the key steps in this common-sense guide include understanding the business's network vulnerabilities, implementing policies to correct security problems, monitoring incoming traffic for suspicious activity, and preparing a response plan in the event of a breach.

44. Unfortunately, cybercrime is on the rise. Globally, thieves and scammers have managed to steal nearly $1 trillion from unsuspecting victims. The cryptocurrency industry is no exception; in fact, the FTC maintains an entire webpage dedicated to helping consumers guard against cybercriminals engaging in fraud concerning cryptocurrency. *See* https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.

45. The prevalence of cryptocurrency theft has increased drastically over the past few years, as more and more investors flood the space. For example, between October 2020 and May 2021 alone, the FTC saw a nearly 1,000% increase in reported losses due to crypto scams compared to the same time period from 2019. *See* https://www.ftc.gov/system/files/attachments/blog_posts/Cryptocurrency%20buzz%20drives%20record%20investment%20scam%20losses/cryptocurrency_spotlight.pdf?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202.

46. Additionally, 2020 saw a staggering increase in losses due to blockchain-linked

[5] Start with Security, Federal Trade Commission, *available at*, https://www.ftc.gov/system/files/documents/plain-language/pdf0205- startwithsecurity.pdf.

hacks; nearly a third of all blockchain-related hacks happened in 2020, resulting in nearly $3.78 billion in total losses. *See* https://atlasvpn.com/blog/blockchain-hackers-stole-3-8-billion-in-122-attacks-throughout-2020.

47. Of these, the vast majority of hacks stole funds from users' private wallet addresses, independent addresses that are not linked to an exchange. Wallet-based theft accounted for over $3 billion of the $3.78 billion stolen in total. *Id.*

48. By contrast, funds maintained on an exchange were relatively well protected; only $300 million (or about 7.9%) of all blockchain-linked funds stolen via hack were stolen from an exchange. *Id.*

49. Since 2020, the trend in cryptocurrency fraud and theft has only gotten worse. The financial service industry saw an 850% increase in account takeovers (a type of fraud where an unauthorized user gains access to an account). *See* https://resources.sift.com/ebook/q3-2021-digital-trust-safety-index-battling-new-breed-account-takeover/.

50. In fact, as of late 2021, cryptocurrency account takeovers have become so prevalent that they account for 39% of all digital fraud. *Id.*

Uphold's Representations

> *"Security is in our DNA. We obsess about it. Our top priority is to protect you, your money, and your information. Uphold is a community. We enforce stringent security standards across our platform – and continually educate our customers on the important role they have to play."*
>
> -- Uphold.com[6]

51. Against this backdrop of fraud, hacks, and account takeovers, Uphold holds itself out to the public as a bastion of data security—a company that takes every precaution to protect

[6] **Exhibit D**, Security, Uphold.com (last accessed February 11, 2022), *available at*: https://uphold.com/en-us/get-started/security.

its users from unauthorized access by scammers and thieves.

52. Specifically, Uphold makes the following representations:

a. "We deploy layered defenses to limit the scope and depth of potential attacks, as well as sophisticated encryption." Ex. D.

b. "Security professionals routinely conduct security audits and penetration testing of our systems." *Id.*

c. "All our providers undergo appropriate due diligence checks. Special attention is paid to integrations incorporating sensitive data." *Id.*

d. "The Uphold team are background checked by an accredited vendor. Mandatory security and privacy training is conducted regularly." *Id.*

e. "The Uphold Security Operations Centre monitors systems year-round and responds immediately to any detected threat." *Id.*

f. "We'll [ ] do email verification if we detect anything untoward. If we detect unusual activity, we'll send you an email to verify it is you." *Id.*

g. Regarding 2-factor authentication: "We give you an extra level of protection in the event that your login and password get stolen or compromised." *Id.*

h. "Uphold is a pioneer in our space when it comes to the security of our consumers: we are one of the first companies working with digital currencies to become certified to PCI/DSS [the Payment Card Industry Security Standards Council], one of the most stringent security standards in the industry. Being compliant means that we are doing our very best to keep our members' valuable information secure and out of the hands of people who could use that data in a fraudulent way." *Id.*

i. "[The Uphold] brand represents our commitment to consumer protection and true

transparent financial services accountability."[7]

53. Together, these representations assure consumers that their funds are safe with Uphold. But this, unfortunately, is not the truth.

54. As Plaintiffs were soon to discover firsthand, Uphold not only fails to live up to these representations, but leaves its users uniquely vulnerable to unauthorized access, failing to properly implement basic security features. To add insult to injury, once an account has been taken over, its original user is left with no option but to watch, in helpless horror, as their funds are stolen away.

Uphold's Two-Factor Authentication

> *"2FA ensures that failure with any of the initial factors or the second factor will prevent access to your online account. So, even if your password is stolen or your phone is lost, the likelihood of someone else having access to your second-factor information is very low."*
>
> -Uphold.com[8]

55. As of the filing of this complaint, it is unknown exactly how unauthorized users gained access to Plaintiffs' Uphold accounts and stole Plaintiffs' cryptocurrency. However, it is known that but for Uphold's failure to properly implement two-factor authentication, Plaintiffs' cryptocurrency would not have been stolen from their Uphold accounts.

56. When Uphold users create an account, they are required to set up two-factor authentication ("2FA"). *See* https://support.uphold.com/hc/en-us/articles/360024041951-Can-you-skip-setting-up-2-factor-authentication-for-your-Uphold-account-?campaignid=15431310198&adgroupid=&adid=&gclid=Cj0KCQiAjJOQBhCkARIsAEKMtO1

[7] **Exhibit A**, Welcome to Uphold. The Internet of Money (Oct. 14, 2015), *available at* https://blog.uphold.com/posts/uphold/welcome-to-uphold-the-internet-of-money.

[8] **Exhibit E**, Improved Two-Factor Authentication: You asked, we listened. Now we're delivering (Feb. 22, 2019), *available at* https://blog.uphold.com/improved-two-factor-authentication-you-asked-we-listened-now-were-delivering#:~:text=2FA%20ensures%20that%20failure%20with,factor%20information%20is%20very%20low.

b5lgXgut77lGlEGijKuBT0PHGhYYuLHZNhNWQ0X8QDC5dBB5IIu0aAj4yEALw_wcB.

57. In 2019, the World Wide Web Consortium and the FIDO Alliance announced the adoption of Web Authentication ("WebAuthn") as a specific standard for authenticators. *See* https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.en.

58. In their combined press release adopting this standard, these industry leaders noted that stolen, weak, or default passwords accounted for 81% of all data breaches. *Id.*

59. 2FA seeks to remedy this problem.

60. As such, 2FA is a minimum industry standard for any financial services company, and is required under New York Law for financial service companies. 23 NYCRR Part 500.

61. 2FA works by implementing a secondary security check whenever a user attempts to login to an online account. Instead of allowing the user to access the account with just their email and password, a 2FA transaction requires the use of an authentication server, which sends a unique code to the user's second-factor device. The user must then confirm their identity by approving the additional authentication from their second-factor device.

62. 2FA can also work by substituting biometrics for the use as a token.

63. Under the PCI/DSS guidelines, with which Uphold purports to be compliant, multi-factor authentication ("MFA"), which requires 2FA or more, is defined as a "[m]ethod of authenticating a user whereby at least two factors are verified. These factors include something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or PIN), or something the user is or does (such as fingerprints, other forms of biometrics, etc.)." *See* https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf?agreement=true&time=1644856213854.

64. Adequate 2FA protections are essential to online security of sensitive accounts,

particularly in a world where account takeovers are rising at such an alarming rate. Whereas user emails and passwords can be compromised fairly easily, access to a 2FA code usually requires that the device be physically in hand at the time of login.

65. Additionally, 2FA codes usually generate once every 30-60 seconds, making them all but impossible to hack using a brute force (number guessing) method.

66. In other words, the primary reason to implement a 2FA security measure is to protect a user's account from unauthorized access, even when the user's email or password has been compromised.

67. However, 2FA is only secure when properly implemented. Proper implementation is not only necessary to comply with industry standards, but it is necessary to comply with the law.

68. 23 NYCRR 500 impacts anyone "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation, or similar authorization under the Banking Law, the Insurance Law, or the Financial Services Law."

69. As a cryptocurrency exchange based in New York, especially as one that requires all of its users to litigate any disputes related to the service under New York law, Uphold is subject to this regulation.

70. Among other things, this regulation requires regulated entities to utilize MFA.

71. MFA compliance requires authentication through verification of at least two of the following types of authentication factors: (1) knowledge (e.g., a password), (2) possession (e.g. a token or text message), and (3) inherence (e.g. biometric data).

72. A system that allows a user with knowledge (but not possession or inherence) to access an account is therefore not compliant with NY law.

73. On December 7, 2021, the New York Department of Financial Services ("DFS")

issued its Guidance on Multi-Factor Authentication, directed at all entities subject to the Department's regulation (including Uphold).[9]

74. According to DFS, "Approximately 64% of Covered Entities that reported Cybersecurity Events from January 2020 to July 2021 had some gap in their MFA. In some cases, MFA was completely absent; in others it was not enabled, misconfigured, only partially implemented, or pending implementation." *Id.*

75. In other words, improperly implemented MFA or 2FA security leaves users vulnerable to account takeover, in violation of consumer expectations and New York law.

76. This is especially true when an organization has an inadequate 2FA recovery method in place.

77. One limitation of 2FA is its inherent reliance on the user retaining physical possession of their registered 2FA device. If a user's 2FA device breaks, or is lost or stolen, that user can no longer access their authenticator, meaning they would be locked out of any account that uses 2FA via that device, unless that user first undergoes the organization's 2FA recovery process.

78. This recovery process allows a user to reset their 2FA device, restoring access to their account.

79. However, if the recovery process is inadequate, a thief can simply pretend to be the accountholder, report the 2FA device as lost, and then bypass the account's 2FA.

80. Therefore, in recovering access to 2FA, an organization should **never** allow a user to use one set of credentials to substitute for another. As the National Institute of Standards and Technology cautioned in its Special Publication 800-63B: Digital Identity Guidelines:

[9] **Exhibit F**, available at https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211207_mfa_guidance#_ftn4.

> The weak point in many authentication mechanisms is the process followed when a subscriber loses control of one or more authenticators and needs to replace them. [. . .] To maintain the integrity of the authentication factors, it is essential that it not be possible to leverage an authentication involving one factor to obtain an authenticator of a different factor.

See https://pages.nist.gov/800-63-3/sp800-63b.html.

81. Compliance with PCI DSS standards similarly requires that authentication methods be fully independent of one another:[10]

> The authentication mechanisms used for MFA should be independent of one another such that access to one factor does not grant access to any other factor, and the compromise of any one factor does not affect the integrity or confidentiality of any other factor. **For example, if the same set of credentials (e.g., username/password) is used as an authentication factor and also for gaining access to an e-mail account where a secondary factor (e.g., one-time password) is sent, these factors are not independent**. Similarly, a software certificate stored on a laptop (something you have) that is protected by the same set of credentials used to log in to the laptop (something you know) may not provide independence.

82. Similarly, PCI DSS compliance requires that authentication factors be conveyed through different channels or networks:

> Where authentication factors are conveyed through a single device/channel—for example, entering credentials via a device that also receives, stores, or generates a software token—a malicious user who has established control of the device has the ability to capture both authentication factors. Transmission of a one-time password (OTP) to a smartphone has traditionally been considered an effective out-of-band method. However, if the same phone is then used to submit the OTP—for example, via a web browser—the effectiveness of the OTP as a secondary factor is effectively nullified. Out-of-band conveyance of authentication mechanisms is an additional control that can enhance the level of assurance for multi-factor authentication. In lieu of the ability to use out-of-band communication, the authentication process should establish controls to guarantee that the individual attempting to use the authentication is, in fact, the legitimate user in possession of the authentication factor.

83. In other words, and unsurprisingly, the 2FA mechanism employed specifically to protect against compromised emails and passwords should not be one that can be reset by gaining

[10] https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf. (Emphasis added).

access to a user's email and/or password.

84. The FIDO Alliance provides specific guidance on appropriate 2FA recovery methods. *See* https://media.fidoalliance.org/wp-content/uploads/2019/02/FIDO_Account_Recovery_Best_Practices-1.pdf. According to this two-step method, the first line of defense is to employ MFA, by which a user registers a backup authentication method in the event of loss of the primary authenticator.

85. However, in the event of a loss of a user's authentication devices, the standard requirement is for the user to undergo identity proofing in accordance with the NIST 800-63A Digital Identity Guidelines. *Id.*

86. This standard (identity proofing) has been broadly adopted across cryptocurrency exchanges. To give a few examples, here is what the highest volume exchanges in the United States do to protect their customer accounts:

a. Coinbase requires the user to provide a photo of the front and back of the user's photo ID, plus a webcam photo of the user taken when prompted by Coinbase. *See* https://help.coinbase.com/en/coinbase/managing-my-account/get-back-into-my-account/2-step-verification-troubleshooting.

b. Binance requires the user to submit a video in which the user faces the camera, holding an ID document, and speaking a statement to verify the user's identity, such as "Today is **DD-MM-YYYY**, I'm applying to reset the **Google/SMS/Email** security verification (2FA) for my account. I confirm that it is my activity, and I am contacting Binance customer service to reset **Google/SMS/Email** security verification for my Binance account **XXXXX@XXXXX.com**." This video must then be submitted along with

a picture of the same ID document depicted in the video. *See* https://www.binance.com/en/support/faq/3ea1490fb94849bbbb445a40ee5e0bd7.

c. Crypto.com requires submission of a video, wherein the user appears holding a piece of paper with that day's full date, the user's full name, and the answers to a number of additional authentication questions; additionally, it requires that the user submit a selfie with specific lighting requirements to protect against digital alterations. *See* https://help.crypto.com/en/articles/3511454-how-do-i-reset-my-2fa.

d. KuCoin requires submission of a photograph of the user holding their ID and a piece of paper with answers to a set of authentication questions, including a code that KuCoin changes daily. *See* https://support.kucoin.plus/hc/en-us/articles/360014897913-Google-2FA#h_894e8d33-aa53-4dec-9272-b52556410dfa.

87. In other words, cryptocurrency exchanges operating according to industry standards employ similar identity-proofing recovery methods.

88. Uphold, on the other hand, does not.

89. In fact, an Uphold user only needs their email address and password in order to recover/change their 2FA device. *See* https://support.uphold.com/hc/en-us/articles/360043633751.

90. With a user's email address and password, a user can prompt Uphold to email the user a code that allows the user to completely remove their old 2FA device and identify a new one. *Id.*

91. From there, a user can quickly make other changes, including changing the

password and even the email address associated with the account, using the codes generated by the newly registered 2FA device.

92. In other words, anyone with access to a user's email and password can remove **the very security measure designed to guard against compromised email and passwords**. This is the same security measure that Uphold told its users existed "in the event that your login and password get stolen or compromised." *See* Exhibit D.

93. Uphold's 2FA device recovery process falls far below the industry standard and leaves Uphold's users effectively as vulnerable to account takeovers as if they did not have 2FA in the first place.

94. That is precisely why this type of 2FA falls squarely outside of industry standards, PCI DSS standards, and New York law.

95. Once a cybercriminal resets a user's 2FA device, they have not only gained full access to a user's Uphold account, but they have also completely blocked the true accountholder from accessing their own account, because the original 2FA can no longer be used to log in. The compromised user is now completely reliant on Uphold's customer support.

Uphold's Customer Support

> *"If you believe that your account has been compromised or hacked, get in touch with us as soon as you can and we'll restrict your account to prevent any withdrawals, until it's fully secured."*
>
> -Uphold.com[11]

96. Until spring of 2021, Uphold represented to users that its Security Operations Center monitored its systems "24 hours a day, 7 days a week, 365 days a year and responds to suspicious activity immediately as it arises."[12]

[11] https://support.uphold.com/hc/en-us/articles/360057752872-I-got-hacked-What-do-I-do-
[12] **Exhibit G**: ARCHIVED VERSION of https://web.archive.org/web/20191129202143/https://uphold.com/en/security-protection/uphold-protecting-you

97. That representation has since been softened to state that the Operations Center "monitors systems year-round and responds immediately to any detected threat."

98. Either way, when users discover a breach to their account's security, they quickly learn that these representations are false.

99. Uphold's customer service is only available by email. There is no fast-track option for serious security breaches such as compromised accounts. There is no way to prioritize a ticket. And there is certainly no way to contact a live individual.

100. This means that if a user becomes aware that their account has been breached (such as by a failure of Uphold's 2FA protocol), the user's only option is to send an email to Uphold. *Id.*

101. Unfortunately, it can take days, and sometimes even weeks, for Uphold's customer support to respond to email requests.

102. On March 14, 2021, Uphold published an article to its website that admitted its customer support was struggling to keep up with user tickets.[13] Among other things, this article stated:

> "We haven't been able to provide anything like the customer service we'd like during this avalanche and recognise that we've let many of you down. We're deeply sorry. We appreciate that there's nothing more annoying than temporary account restrictions and slow response times."
>
> "We'd like to explain the challenges we've faced and how we're turning the page over the next few weeks to introduce a vastly-improved customer experience."
>
> "Like other crypto platforms, we've seen dramatic spikes in both sign-ups and trading activity that have deluged our already-busy teams. Adding and training extra support staff quickly enough - a challenge in the best of times - has proven to be doubly difficult during lockdown."
>
> "We've also suffered from inefficiencies created by legacy fraud and compliance policies and systems that, in normal times, are constantly contending with the advancements of scammers and bad actors, but were not optimized to cope with the 50x

[13] **Exhibit H**, available at https://support.uphold.com/hc/en-us/articles/360057035232-Improving-our-customer-support.

increase in volumes we've seen."

> "The result has been a backlog of tickets that has clogged up our system and created unacceptable wait times for you. We're taking action to make sure this never happens again."

103. But many of the actions Uphold took were, instead, cost-saving measures designed to sacrifice security in favor of increasing efficiency. Among other things, Uphold announced several key changes.

104. Uphold would halve the total number of times when its automated monitoring services froze accounts for suspicious activity: "We're slashing the number of situations in which we restrict your account - in fact, we're cutting it by almost half - as we reward lower-risk customers for good standing." *Id.*

105. Uphold would introduce automated email address and 2FA reset options: "You'll have to contact customer service less because you'll be able to self-serve in the app for things like changing your email address or 2-factor authentication, without needing any help from us." *Id.*

106. Uphold would allow users to "correct" key identifying information, such as their date of birth, without triggering an account restriction: "We're introducing rules that mean if you make a mistake in your declared info - such as a digit wrong in your date of birth - you can correct it without having your account restricted." *Id.*

107. Uphold would eliminate the use of authenticators for approved devices: "Our clunky 2-factor authentication Security measures - which require you to use a third-party app - are being scrapped and replaced with face-recognition technology for supported devices on our mobile app." *Id.*

108. One of the only changes Uphold announced that would have actually mitigated security risks was the introduction of telephone-based support; prior to March 14, 2021, there was

no option to contact Uphold by phone, which meant users had no option for immediate recourse if they suspected their account had been compromised.

109. As of today, there is still no telephone support option available.

110. As a result, by the time users receive a response from Uphold regarding their compromised accounts, it is far too late to stop the cybercriminals from stealing their funds and personal information.

111. This is far below the usual standard for this industry. By way of contrast, here is how the top cryptocurrency exchanges that offer a customer support line:

a. Coinbase provides a phone number: 1-888-908-7930 (connects users to an automated system that will allow them to freeze their accounts immediately if they suspect the account has been compromised);

b. Binance.us offers users the ability to self-disable their accounts immediately, which also cancels all pending transactions and withdrawals. Users unable to self-disable (such as those no longer able to login) can use the virtual assistant to quickly disable their accounts;

c. Kraken provides live customer support by phone;

d. KuCoin allows users to freeze their own accounts by following a link; and

e. Crypto.com uses an in-app chat.

112. To make matters worse, when Uphold finally responds to its users' requests, it places their accounts "under review"—during which time the user is unable to complete any transactions whatsoever.

113. This review process can take months, if not longer. In the meantime, users cannot

even withdraw any remaining funds from their accounts. For some users, this months-long process is still unresolved, with no end in sight.

114. Adding insult to injury, the result of Uphold's own investigation is always, or virtually always, to cast blame on the user, rather than acknowledging any pitfalls in its own system.

115. Specifically, this internal investigation determines that Uphold is not to blame for the account takeover, and that the accountholder's email address must have been compromised.

116. Even if this were true, this finding of a compromised email account would ignore the fact that compliant 2FA implementation would still have prohibited a cybercriminal from accessing a user's Uphold account, as discussed above.

117. When they learned of the account takeover, many victims, like Plaintiffs, contacted their email providers and internet service providers (ISPs) to determine whether there had been any suspicious activity associated with their accounts.

118. Neither the email providers nor ISPs had any record of logins from unusual IP addresses or geolocations.

119. Even more appallingly, many victims were not automatically logged out of the mobile application when these login changes went into effect. This means that once a cybercriminal gains access to an Uphold account, changing one's login credentials will not terminate that cybercriminal's access.

120. On information and belief, some victims learned this the hard way, when they received a notification that there were transactions in their account that they did not authorize, causing them to immediately log in and change their password. However, on information and belief, in such scenarios, the cybercriminal stole funds from victims' accounts even **after** these

victims had changed their passwords.

121. Uphold has consistently blamed all or virtually all victims for the losses in their accounts, suggested they contact their local authorities, and refused to refund any of the cryptocurrency that had been stolen.

122. In other words, Uphold presents itself as a highly secure cryptocurrency exchange, exposes its users to significant risks that fall far below the industry standard for security, fails to respond to time-sensitive incidents such as account takeovers, and then ultimately refuses to accept responsibility for the myriad failings in its own system.

123. What is more, Uphold encourages users seeking to reset their passwords to contact its support team if they "have completely forgotten" the email address they used to sign up or if they "lost" their security key or "have no access" to their 2FA code. *See* https://support.uphold.com/hc/en-us/articles/202778058-How-to-update-change-or-reset-your-password. In other words, it invites social engineering attacks by allowing customer support members to grant access to accounts even when a user lacks access to the original email or 2FA device.

124. Upon information and belief, numerous unauthorized users have gained access to Uphold accounts by taking advantage of Uphold's failure to properly implement 2FA and Uphold's severely understaffed customer service team.

125. In other words, the same customer support team that leaves bona fide users to fend for themselves against account takeovers actually plays a role in facilitating these same takeovers in the first place.

Summary of Security Lapses

126. Uphold leaves its users vulnerable in several ways. While Plaintiffs reserve the right

to amend this Complaint as discovery makes new facts available, at this time they are aware of at least seventeen ways Uphold fails its users.

127. Uphold allows users to reset 2FA devices with only an email account and password, and without requiring users to prove their identities. This failure renders Uphold's 2FA meaningless.

128. Uphold invites users to change key account information by contacting customer support, inviting social engineering attacks.

129. Uphold halved the number of situations where its monitoring system would automatically freeze or disable accounts due to suspected fraudulent activity. This means that accounts are not automatically frozen even when they are accessed from an unrecognized IP, in an unrecognized geolocation, followed by an immediate change of a user's password, authentication device, and email, thereby allowing the transfer of funds out of the user's account to a wallet the user has never used before.

130. Uphold fails to provide users a way to freeze their own accounts.

131. Uphold fails to provide a phone number, online tool, or priority support option for users to freeze their accounts by contacting support.

132. Uphold fails to sufficiently staff its customer support team to process account freeze requests.

133. Uphold allows anyone logged into its mobile application to remain logged in, even after a user changes account access information.

134. Uphold fails to send timely notice of account changes via email, as promised.

135. Upon receiving notice of countless users reporting account takeovers, Uphold failed to take any action to mitigate security risks to other users, over a period of months.

136. Uphold failed to notify its users of these cybersecurity risks.

137. Uphold failed to audit its own cybersecurity in light of these user reports.

138. Uphold failed to migrate its users away from SMS-based 2FA. While Uphold requires newly registered users to utilize a third-party authenticator, users who signed up prior to this requirement have been allowed to keep their original SMS authentication method. This is an inferior authentication method that leaves users vulnerable. Upon information and belief, Uphold has never explained this vulnerability to its pre-existing user base or invited them to upgrade their security.

139. Upon information and belief, Uphold has failed to report cybersecurity incidents to applicable regulatory bodies.

140. Uphold does all of this while actively misleading users into believing it is a secure cryptocurrency exchange, and misrepresenting the strength of its security protocols.

141. Uphold holds itself out to the public as a New York company, imposing New York law on its users in connection with their use of the service, and causing them to trust that it is subject to New York's regulations, all without possessing a BitLicense as required to operate as a cryptocurrency exchange under New York law.

142. Uphold holds itself out as PCI DSS certified, deceiving consumers into believing their accounts will be secured to the highest standard, when in fact its MFA methods are non-compliant with PCI DSS requirements.

143. These failures left Plaintiffs and the other Class Members exposed to a number of potential scenarios, each of which would have been avoided had Uphold properly implemented 2FA and the other security measures described above.

144. **Scenario 1:** As an example, and upon information and belief, some unauthorized

users gained access to Uphold accounts by obtaining access to actual account holders' email accounts.

145. From there, an unauthorized user was able to use Uphold's account recovery protocols to remove or change the 2FA device connected with an account.

146. The unauthorized user was able to change the 2FA device without access to the original device and without proving their identity.

147. Once they updated the 2FA device associated with an account, the unauthorized user used the codes that their counterfeit 2FA devices generated to effect a number of changes to the account's credentials, blocking the original user from the account.

148. From there, the unauthorized user was able to transfer funds out of the Uphold account.

149. Had Uphold implemented proper 2FA, an unauthorized user would not have been able to log into and transfer funds out of an Uphold account, even when the unauthorized user had obtained access to the account holder's email account.

150. **Scenario 2:** Upon information and belief, some unauthorized users gained access to Uphold accounts by obtaining account holders' Uphold login information, and then mimicking a recognized IP address so that Uphold did not require 2FA upon login.

151. Once logged in, the unauthorized user reviewed the account information and impersonated the actual account holder to Uphold customer support and requested that customer support reset the 2FA device.

152. Had Uphold implemented proper 2FA, it would not have been possible for an unauthorized user to log into an Uphold account or change 2FA device through customer support as a new code would have been required on login.

153. **Scenario 3:** Upon information and belief, some unauthorized users gained access to Uphold accounts by taking advantage of the fact that Uphold failed to require users who signed up prior to the implementation of 2FA to update their accounts.

154. Such users did not have 2FA in place. As a result, if an unauthorized user gained access to such a user's username and password, or to their email address, the unauthorized user could simply install a new 2FA device.

155. Had Uphold implemented proper 2FA for all users, it would not have been possible for unauthorized users to log into the Uphold account without 2FA.

156. **Scenario 4:** Upon information and belief, some unauthorized users gained access to Uphold accounts by taking advantage of insecure SMS-based authentication.

157. Uphold previously allowed users to authenticate by SMS. New users must use a third-party authenticator app. However, Uphold never required its existing users to update their authentication method.

158. SMS-based authentication is vulnerable to numerous vulnerabilities, including SIM card swapping. This allows an unauthorized user to mimic the true user's phone number, and intercept authentication codes.

159. Had Uphold properly enforced a third-party authenticator requirement, it would not have been possible for an unauthorized user to log into an Uphold account without 2FA connected to a third-party authenticator app.

160. **Scenario 5:** Upon information and belief, some unauthorized users gained access by orchestrating social engineering attacks.

161. Indeed, Uphold has a history of exposing its users to such thefts.

162. Despite assuring customers that all of its employees undergo background checks,

including criminal background checks, Uphold's affiliated entity, Uphold Europe Limited, hired Sameer Ismail as its Chief Compliance Officer, despite the fact that Mr. Ismail had a prior conviction for theft.

163. Uphold Europe Limited admitted in court pleadings that Mr. Ismail took actions (including with respect to accounts held by Uphold HQ Inc.'s users) to defraud customers.

164. Among other things, Mr. Ismail was able to disable 2FA on these accounts.

165. Mr. Ismail also specifically changed the accounts' email addresses in order to prevent the customers from getting notices about changes to their accounts.

166. Mr. Ismail stole nearly $500,000 from various users, including Uphold users, using these methods.

167. Upon information and belief, customer service representatives today have the same account changing capabilities as Mr. Ismail. That is, they can add and remove 2FA devices, change emails, etc.

168. Upon information and belief, some unauthorized users gained access to customer accounts by working with compromised Uphold employees to effect changes.

169. Such misconduct would explain why certain users, such as Plaintiff Smith, received no notifications about the changes to their accounts.

170. Had Uphold properly implemented 2FA, it would not have been possible for a customer service representative to unilaterally remove a 2FA device without first undergoing strenuous internal checks and verifications, which would make this sort of fraud impossible.

Plaintiff Theodore Rider

171. Plaintiff Rider created his Uphold account in February 2021, and later he set up two-factor authentication with his Google Authenticator app. He used the same Authenticator app

for his accounts held at Coinbase, Coinbase Pro, and Robinhood, and he has never had any security problems with any account other than Uphold. Despite having other accounts, he held most of his life savings in his Uphold account.

172. On Friday, November 12, 2021, Rider checked the balance in his Uphold account, which was over $22,437 just days before. However, when he launched the Uphold mobile app, he could not gain access to his account. When he eventually determined that his two-factor authentication had been reset without his permission, he broke out into a cold sweat and was in shock.

173. Rider immediately contacted Uphold in every way he could, including on Twitter, Reddit, Facebook, and Instagram, in addition to emailing Uphold customer support. He even left a voicemail on a general telephone mailbox that explicitly said it was not a customer service line. Each time he informed Uphold that his account may have been compromised and to stop all transactions in the account, with messages like, "ATTENTION: My account has been compromised. Please stop any and all transactions and withdrawals, IMMEDIATELY!" He did not get a "ticket number" from Uphold until Monday, November 15, 2021, which was by email, and it was only then that Uphold "froze" his account, stopping all further transactions. On November 18, 2021, Uphold finally allowed Rider to access his Uphold account, at which time he discovered that the account had a zero balance.

174. While Rider was waiting for Uphold to respond to his requests to freeze his account after his November 12, 2021 communications to Uphold, all of Rider's cryptocurrency was transferred out of his account prior to Uphold freezing his account on November 15, 2021; in addition, between November 12 and 15, 2021, someone had initiated ACH transactions from

within Rider's Uphold account, completely depleting Rider's bank account and causing an overdraft of $2,500.

175. During this pivotal three-day period between when Rider first notified Uphold of the unauthorized access to his account, and when Uphold finally froze his account, Rider's messages became increasingly desperate, due to Uphold not confirming that it would freeze the account and Rider not being able to log in to his account to see what was happening: "…but no one is allowing me to access my uphold account & no one is showing me or even assuring me that my cryptos are still there or are being recovered. I'm still locked out & my whole life is on uphold! I need help! Please try to put yourself in my situation. What if all your money was suddenly gone? Wouldn't you want help??" Unfortunately, Uphold ignored Rider's pleas and missed an opportunity to stop the theft of Rider's life savings.

176. When Uphold finally responded to Rider, Uphold glibly stated that someone had changed his email address on record in his Uphold account, and thereafter changed his password, and thereafter changed his two-factor authentication device, despite the fact that Rider was never notified of any of these changes.

177. Uphold denied all responsibility for the theft and suggested that Rider file a report with his local police department.

178. Had Uphold implemented proper 2FA with respect to Rider's account, the unauthorized user would not have been able to transfer Rider's cryptocurrency out of Rider's Uphold account.

Plaintiff Jesse Smith

179. Plaintiff Jesse Smith is an active-duty service member of the U.S. Navy, currently stationed in North Carolina, where he lives with his wife of 15 years and their two daughters.

180. Smith created his Uphold account in December of 2020, and he set up two-factor authentication with an authenticator app at that time.

181. Smith regularly checked his Uphold account. He had set up his phone to receive as many Uphold notifications as possible, including marketing messages, market fluctuation alerts, and security notifications.

182. On October 5, 2021, Smith opened his Uphold mobile application to discover his account showed a zero balance, despite the fact that he had been holding $12,000 worth of XRP in his account.

183. He navigated to his account history, which showed that someone using an IP address located in Turkey had converted all of his XRP into Tether ("USDT"), then to Ethereum ("ETH"), before transferring it to an unknown wallet address on another cryptocurrency exchange.

184. Smith had never received a single notification from Uphold about these transactions.

185. From within the Uphold app, Smith noticed that his account's email address of record had been changed to an Outlook email that he did not recognize.

186. Smith immediately contacted Uphold via online chat and was instructed to send an email to customer support.

187. Uphold froze Smith's account a few hours later—long after the damage had already been done.

188. Smith contacted his email service provider and his mobile phone provider, both of which confirmed there was no evidence of unauthorized or suspicious activity in Smith's email account or on his phone.

189. Smith contacted his email provider, Yahoo!, within seven days of the date when

changes were first made to his Uphold account.

190. Yahoo! allows users to restore lost or deleted emails from within the previous seven days, provided the user submits a restore request. *See* https://help.yahoo.com/kb/SLN2552.html#:~:text=Messages%20can%20only%20be%20restored,you%20pick%20to%20restore%20to. Smith did just that. His account showed that no messages had been deleted, and he had not received any emails from Uphold notifying him of any changes that had been made to his account.

191. Meanwhile, the cybercriminal had not only infiltrated Smith's Uphold account, they had successfully changed his password, his 2FA device, the email address associated with his account, and had transferred his cryptocurrency to an external wallet.

192. All of these actions should have triggered email notifications under Uphold's system. But apparently, none of them did.

193. To this day, Smith is able to access his account using the Uphold mobile application, even though the account email, password, and authentication device have all been changed. He can no longer login via the Uphold website.

194. From within his Uphold account, Smith can see IP activity that shows the cybercriminal accessed his account from an IP address in Turkey.

195. Shockingly, this unusual login activity, coupled with rapid-fire changes to the account authenticator, password, and email, did not trigger Uphold's alleged 24/7 security monitoring service to flag or freeze Smith's account.

196. Even more appallingly, Smith was not automatically logged out of the mobile application when these login changes went into effect. This means that once a cybercriminal gains access to an Uphold account, changing one's login credentials will not terminate that

cybercriminal's access.

197. Uphold nevertheless denied any responsibility for Smith's loss.

198. To this day, Smith's account remains frozen. The fraudulent email is still listed as the primary email address within Smith's account, and Smith has been unable to recover any of the funds that were stolen from him.

199. Smith and his family had hoped that $12,000 could be put towards a down payment for their first home. Now, those hopes have been dashed.

200. Had Uphold implemented proper 2FA with respect to Smith's account, the unauthorized user would not have been able to transfer Smith's cryptocurrency out of Smith's Uphold account.

Plaintiff Gilles Boevi

201. Plaintiff Gilles Boevi lives in Hoboken, New Jersey, where he works as a senior customer engineer for Microsoft Corp US.

202. Boevi created his Uphold account on April 13, 2021, at which time he set up two-factor authentication using Microsoft's Authenticator app.

203. Boevi spends his days working with computers, and he is no stranger to the importance of cybersecurity. He felt comfortable keeping his cryptocurrency on Uphold because he understands how two-factor authentication works, and knew it would be impossible for a thief to steal his funds without physical access to his phone.

204. When Boevi lost his $26,176.21 of cryptocurrency, as described above, it caused him tremendous emotional distress. He had been planning to move with his girlfriend to Florida, using the funds he held with Uphold to finance the move. With the money gone, those plans vanished.

205. The situation has caused Boevi significant emotional distress, to the point that he has had to obtain medical care.

206. Had Uphold implemented proper 2FA with respect to Boevi's account, the unauthorized user would not have been able to transfer Boevi's cryptocurrency out of Boevi's Uphold account.

Plaintiffs' Damages

207. Plaintiffs seek redress for the significant damages they and all Class Members suffered as a result of Uphold's misconduct in failing to maintain the integrity of its users' accounts.

208. As a result of this misconduct, Plaintiffs, and other members of the putative class, have been damaged, including, but not limited to, in the following ways:

a. The theft of their cryptocurrencies;

b. The loss of funds from personal bank accounts due to unauthorized ACH transactions initiated by bad actors from within customer accounts;

c. The theft of personal and financial information stored in connection with their Uphold user accounts (which includes, in some instances, bank account information and access);

d. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts in the future;

e. Damages arising from the inability to use their accounts to recover any remaining funds and/or sell their cryptocurrencies during all-time high pricing;

f. Time spent and costs associated with loss of productivity and/or enjoyment of life from taking time to address, ameliorate, and mitigate the actual

and future consequences of these account takeovers;

g. Stress, anxiety, depression, and other emotional damages resulting from the incident and prolonged efforts to obtain a response from Uphold;

h. The imminent and impending injury flowing from the risk of fraud and identity theft related to the theft of their private information; and

i. Their loss of privacy.

CLASS ACTION ALLEGATIONS

209. Plaintiffs bring this class action pursuant to Federal Rules of Civil Procedure ("Rule(s)") 23(a) and 23(b)(3) and seeks certification of the class as identified below.

Definition of Proposed Class

210. Plaintiffs bring this class action on behalf of the following class (the "Class"):

> All persons who created an account on the Uphold cryptocurrency exchange and who had their funds stolen after someone else removed an existing 2FA device and/or installed a new 2FA device. Excluded from the Class are Defendants and their officers and directors at all relevant times, members of Defendants' immediate families and their legal representatives, heirs, successors, and assigns, and any entity in which the Defendants have or had a controlling interest.

211. Plaintiffs reserve the right to amend or modify the Class in connection with a Motion for Class Certification or as the result of discovery.

212. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as individual Class Members would use to prove those elements in individual actions alleging the same claims.

Size of the Proposed Class

213. Plaintiffs do not currently know the exact size of the proposed Class. However,

Plaintiffs are aware that the Class is so numerous that joinder of the individual Members of the proposed Class is impracticable. On information and belief, the Class includes at least thousands of people throughout the world. The number and identities of Class Members are unknown to Plaintiffs, but can be ascertained through discovery, including into Uphold's account records, electronic messages, and customer service files, as well as through published notice.

Adequacy of Representation by the Class Representative

214. Plaintiffs' claims are typical of the Class, and Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no interests adverse to the interests of the Class and have retained counsel with experience in the prosecution of class actions and complex litigation, including consumer litigation, and who will vigorously prosecute this action.

Common Questions of Law and Fact

215. Questions of law or fact common to the Class exist as to Plaintiffs and all Class Members, and these common questions predominate over any questions affecting only individual Class Members. Among the common questions of law and fact are the following:

a. The extent of user reports of account takeovers;

b. Defendants' efforts, if any, to prevent unauthorized access to its users' accounts;

c. The extent to which Defendants failed to abide by industry standards in implementing 2FA measures;

d. Defendants' knowledge of account takeovers and their response to the same;

e. Defendants' training, protocols, and security measures taken with respect to its customer service team;

f. Defendants' internal guidelines for when an account should be frozen;

g. Defendants' compliance (or lack thereof) with regulatory cybersecurity and reporting requirements;

h. Whether Defendants' conduct constituted a breach of contract;

i. Defendants' warranty obligations to Plaintiffs and the Class;

j. Whether Defendants owed Plaintiffs and the Class a fiduciary duty, and whether they breached the same; and

k. The amount of damages sustained by Plaintiff and the Class.

Typicality of Claims of the Class Representatives

216. Plaintiffs do not anticipate any difficulties in the management of this action as a class action. The Class is ascertainable, and there is a well-defined community of interests in the questions of law and fact alleged because the rights of each Class Member were violated in similar fashion based on Defendants' misconduct. Notice can be provided through records and publication, the cost of which is properly imposed upon Defendants.

217. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs and the Class Members. Common questions of law and fact predominate over any individual questions that may arise.

218. The injuries sustained by Plaintiffs and the Class Members flow, in each instance, from a common nucleus of operative facts, *i.e.*, Defendants' contractual promise and implied warranty to provide security measures at least in accordance with industry standards, without defects, and Plaintiffs' and the Class Members' damages resulting from Defendants' failure to provide these adequate security measures.

219. Plaintiffs' claims are typical of the claims of the Class they seek to represent. Defendants' uniform obligations relating to its cryptocurrency exchange services apply equally to Plaintiffs and all Class Members. Moreover, the defenses, if any, that will be asserted against Plaintiffs' claims are typical of the defenses, if any, that will be asserted against all Class Members' claims (*e.g.,* that the account takeovers were not caused by Defendants).

Nature of the Notice to the Proposed Class

220. Plaintiffs know of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action. The vast majority of the names and contact information of the Class Members is likely available from Defendants or their partners.

221. The class definition is carefully drawn such that the Class Members can easily be identified and notified using standard class notification methods, including analysis of Defendants' sales records, mailing, electronic notification, and other methods.

222. To the extent possible, Plaintiffs contemplate providing notice(s) to the Class, as approved by the Court, through the mail or as otherwise directed. In the alternative or in connection with mailed notices, Plaintiff may utilize paid advertising notices online or in media likely to draw the attention of Class Members *e.g.*, specialty magazines. The notice(s) shall, among other things, advise the Class that they shall be entitled to "opt out" of the Class if they so request by a date specified within the notice and that any judgment, whether favorable or not, entered in this case will bind all members except those who affirmatively exclude themselves by timely opting out.

Additional Matters Pertinent to the Findings as

Provided by Fed. R. Civ. P. 23(b)(3)

223. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, and individual joinder of all Class Members is impracticable, if

not impossible, because the massive number of Class Members are scattered throughout the world. Moreover, the cost to the court system of such individualized litigation would be substantial. Individualized litigation would likewise present the potential for inconsistent or contradictory judgments and would result in significant delay and expense to all parties and courts hearing virtually identical lawsuits. By contrast, the conduct of this action as a class action would present fewer management difficulties, conserve the resources of the parties and the courts, and protect the rights of each Class Member and maximize recovery to them.

224. Given the amount in controversy for each individual Member of the Class, the relief sought in this case, that Defendants have acted on grounds generally applicable to the entirety of the Class, and the large size of the anticipated Class, the interest of each Class Member in controlling his or her own case is relatively low; there are relatively minimal expected difficulties likely to be encountered in managing a class action; Plaintiffs anticipate that relevant foreign courts will recognize a United States judgment in this case; Plaintiffs are not aware of other litigation by individual Class Members already in progress involving the same controversy; Uphold has required that Plaintiffs and all Class Members litigate under New York law; and there is a strong desirability of consolidating all claims in a single action before a single court in the United States.

FIRST CAUSE OF ACTION

(Negligence)

225. Plaintiffs incorporate by reference all of the above allegations as if fully set forth herein.

226. Plaintiffs bring this claim on behalf of themselves and the Members of the proposed Class.

227. Upon accepting and storing Plaintiffs' private information and cryptocurrency on

its service, Uphold undertook and owed to Plaintiffs and the Class members a duty to exercise reasonable care to secure and safeguard access to the information and funds contained in these accounts.

228. Uphold owed a duty of care not to subject Plaintiffs and the Class Members to an unreasonable risk of harm, because they were the foreseeable and probable victims of any inadequate security practices.

229. Uphold owed numerous other duties to Plaintiffs and the Class Members, including the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, disabling, freezing, and protecting its users' accounts;

b. To implement adequate security procedures and systems which were compliant with industry-standard practices;

c. To implement procedures designed to quickly detect a security breach and to timely act on reports of security breaches;

d. To update its security protocols and procedures upon receiving notice of vulnerabilities within its security system; and

e. To adequately staff security teams in order to ensure the integrity of user accounts upon report of a breach.

230. Uphold also owed Plaintiffs and the Class Members duties under New York law, including a duty to properly implement MFA under 23 NYCRR 500 and to maintain a BitLicense under 23 NYCRR 200. Uphold breached these duties.

231. Uphold further breached its statutory duties designed to protect members of the public from harms caused by data breaches, including but not limited to using reasonable measures

to protect private information, as imposed by Section 5 of the Federal Trade Commission Act (the "FTCA").

232. Uphold also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard their accounts by knowingly disregarding standard information security principles, despite obvious risks.

233. These breaches evince a reckless disregard for the rights of Plaintiffs and the Class Members. Uphold did not exercise even slight care in attempting to meet its various duties.

234. As a result of Uphold's breaches, cybercriminals were able to gain unauthorized access to Plaintiffs' and the Class Members' accounts.

235. Uphold knew, or reasonably should have known, of the risks inherent in keeping and storing cryptocurrency on its exchange on behalf of users, the vulnerabilities of its systems, and the importance of having adequate data security measures in place.

236. Uphold knew, or should have known, that its security measures did not adequately safeguard Plaintiffs' and the Class Members' accounts from unauthorized access.

237. Uphold had a special relationship with Plaintiffs and the Class Members. Their willingness to entrust Uphold with their cryptocurrency and personal information was predicated on the understanding—one strengthened by Uphold's own representations—that Uphold would take adequate security measures. Moreover, only Uphold had the ability to protect its systems with the appropriate security measures to protect users from cybercriminals.

238. Uphold's conduct created a foreseeable risk of harm to Plaintiffs and the Class Members, in that it created conditions conducive to a foreseeable, intentional criminal act: namely, the unauthorized access of their accounts and personal information.

239. As a direct and proximate cause of Uphold's conduct, Plaintiffs and the Class

Members have suffered, and will continue to suffer, damages and injury, including the loss of their cryptocurrency, theft of their personal information, anxiety, emotional distress, loss of privacy, and other economic and other non-economic losses, plus interest and attorney's fees, in an amount to be proven at trial.

240. Additionally, due to Uphold's gross negligence in the performance of its various duties, Plaintiffs and the Class Members are entitled to recover punitive damages.

SECOND CAUSE OF ACTION

(Negligence *per se*)

241. Plaintiffs incorporate by reference all of the above allegations as if fully set forth herein.

242. Section 5 of the FTCA bars unfair and deceptive acts and practices "in or affecting commerce," which the FTC has interpreted and enforced as including action against organizations that have misled consumers through a failure to maintain appropriate security for sensitive information.

243. Uphold violated Section 5 of the FTCA in its failure to implement reasonable security measures and in its abandonment of industry standards regarding the protection of its users' private information.

244. Uphold additionally violated the FTCA by misrepresenting the strength, character, and nature of its security measures, and by holding itself out to the public as compliant with PCI DSS security standards—when, in fact, it is not.

245. This conduct was materially misleading in that it would cause a reasonable consumer to believe that Uphold not only employed industry standard security measures, but in fact utilized more robust security protocols, as necessary to comply with PCI DSS standards.

246. Uphold also materially misled consumers into believing that it monitored their accounts for potential fraud 24/7, when in fact it did not.

247. It also materially misled customers into believing they would be able to contact its customer support team immediately if their account became compromised, when in fact they could not.

248. Additionally, as a money services business, Uphold has strict compliance obligations under the Currency and Foreign Transactions Reporting Act of 1970, aka the Bank Secrecy Act ("BSA") to monitor customer transactions and report any suspicious activities to law enforcement authorities. *See* 31 U.S.C. §5311; 12 C.F.R. §208.63.

249. Uphold failed to meet these reporting obligations.

250. As a result of these material misrepresentations and reporting failures, Plaintiffs and the Class Members were lured into creating accounts on Uphold and using them to store their cryptocurrency, when they otherwise would not have.

251. And, as a direct and proximate result of Defendants' misleading statements, Plaintiffs and the Class Members lost money and privacy when Defendants' failure to live up to their promises allowed cybercriminals to takeover and deplete Plaintiffs' and the Class Members' accounts.

252. The harm suffered by Plaintiffs and the Class Members as a result is the type of harm the FTCA was intended to safeguard the public against.

253. As a direct and proximate cause of Uphold's negligence *per se*, Plaintiffs and the Class Members have suffered, and will continue to suffer, damages and injury, including the loss of their cryptocurrency, theft of their personal information, anxiety, emotional distress, loss of privacy, and other economic and other non-economic losses, plus interest and attorney's fees, in

an amount to be proven at trial.

THIRD CAUSE OF ACTION

(Violations of New York Consumer Law for Deceptive Acts and Practices)

N.Y. Gen. Bus. Law 349

254. Plaintiffs incorporate by reference all of the above allegations as if fully set forth herein.

255. New York General Business Law ("NYGBL") 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

256. This law applies to all consumer disputes with respect to their use of Uphold's website and services, both because Uphold is headquartered in New York and because it binds all its users to resolve disputes under New York law, without regard for conflict of law provisions.

257. As alleged herein, Uphold engaged in several unlawful practices, including (but not limited to) the following:

a. Operating as a New York cryptocurrency exchange without a BitLicense, in violation of 23 NYCRR 200;

b. Failing to implement MFA which complied with the provisions of 23 NYCRR 500; and

c. Violating Section 5 of the FTCA as set forth above.

258. Additionally, Uphold violated NYGBL 349 by misrepresenting, both by affirmative representation and by omission, the safety of its systems and services, specifically including (but not limited to) the following:

a. The safety and adequacy of its 2FA method;

b. Its compliance with PCI DSS standards;

c. Its use of a 24/7 monitoring system that would automatically freeze accounts in the event of suspicious activity;

d. The availability of customer service options to freeze an account upon a breach by a cybercriminal; and

e. Uphold's compliance with industry standard security specifications.

259. Uphold also violated NYGBL 349 in that it failed to give timely warnings and notices regarding known defects and problems with the security systems it maintained to protect Plaintiffs' and the Class Members' accounts.

260. Uphold also violated NYGBL 349 by failing to implement reasonable and appropriate security measures or to adequately follow industry standards for data security, and by failing to immediately take action to secure compromised accounts upon receiving notice of the same. If Uphold had complied with these requirements, Plaintiffs and the Class Members would not have suffered the damages they experienced.

261. This conduct, collectively and individually, constitutes an unconscionable commercial practice, in that Uphold has, by the use of false statements and/or material omissions, failed to properly represent and/or has concealed its defective security measures and procedures.

262. Members of the public, including Plaintiffs and the Class Members, were deceived by and relied upon these misrepresentations.

263. Such acts were material, in that they were likely to mislead a reasonable consumer into maintaining an account with Uphold and storing cryptocurrency on its exchange.

264. These acts were consumer-oriented, in that Uphold specifically marketed to consumers regarding its state-of-the-art security measures.

265. These acts caused Plaintiffs and the Class Members to suffer consumer-related injuries by causing them to incur actual and future losses of cryptocurrency.

266. These damages were directly and proximately caused by Uphold's conduct as described herein.

267. In addition to, or in lieu of, actual damages, Plaintiffs and the Class Members seek statutory damages for each injury and violation which has occurred.

FOURTH CAUSE OF ACTION

(Unjust Enrichment)

268. Plaintiffs incorporate by reference all of the above allegations as if fully set forth herein.

269. Plaintiffs bring this claim on behalf of themselves and the Members of the proposed Class.

270. Plaintiffs and the Class Members conferred a monetary benefit on Uphold. Specifically, they paid fees and commissions to purchase, exchange, and sell cryptocurrencies on Uphold's exchange.

271. In exchange, Plaintiffs and the Class Members should have received the goods and services that were the subject of their transactions, including the protection of their accounts with adequate data security.

272. Uphold knew that Plaintiffs and the Class Members conferred a benefit on them and has accepted or retained that benefit. Uphold profited from Plaintiffs' cryptocurrency transactions and used Plaintiffs' and the Class Members' private account information for business purposes.

273. Uphold failed to secure Plaintiffs' and the Class Members' accounts and, therefore,

did not provide full compensation for the benefit Plaintiffs' and the Class Members' use of its services provided.

274. Uphold acquired its fees and Plaintiffs' and the Class Members' private information via inequitable means, as it failed to disclose the inadequate security practices as alleged herein.

275. If Plaintiffs and the Class Members knew that Uphold would not adequately secure their accounts, they would not have transacted on Uphold's website and mobile application, nor conferred to Uphold the benefit of their fees.

276. Plaintiffs and the Class Members have no adequate remedy at law.

277. Under the circumstances, it would be unjust for Uphold to be permitted to retain any of the benefits Plaintiffs and the Class Members conferred on them.

278. Uphold should therefore be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and the Class Members, all proceeds which it unjustly received from them.

279. In the alternative, Uphold should be compelled to refund the amounts that Plaintiffs and the Class Members overpaid.

FIFTH CAUSE OF ACTION

(Breach of Contract)

280. Plaintiffs incorporate by reference all of the above allegations as if fully set forth herein.

281. Plaintiffs bring this claim on behalf of themselves and the Members of the proposed Class.

282. Plaintiffs and the Class Members entered into written contracts with Uphold. These include Uphold's Terms of Service, attached as **Exhibit C**, and its Privacy Policy, attached as

Exhibit I.

283. In addition to the terms contained in these contracts, Uphold was bound by the covenant of good faith and fair dealing, which is inherent to any contract.

284. As more fully described above, Uphold breached its contracts with Plaintiffs and the Class Members by failing to properly secure their accounts against unauthorized access by a cybercriminal.

285. Uphold promised to consumers on its website, mobile application, promotional materials, and in its blog articles, that it was an industry leader in ensuring account security, that it was PCI DSS compliant, and that it employed numerous safeguards to protect against unauthorized account access.

286. Additionally, it promised that it monitored user accounts for suspicious activity and immediately suspended accounts once suspicious activity occurred, and that it would take immediate action if consumers notified it that their accounts had been breached.

287. Plaintiffs and the Class Members have performed all covenants and conditions required under their contracts with Uphold, and/or have been excused from doing so as a result of Uphold's breach.

288. As a direct and proximate cause of Uphold's breach, Plaintiffs and the Class Members have suffered, and will continue to suffer, damages and injury, including the loss of their cryptocurrency, theft of their personal information, and other economic losses, plus interest and attorney's fees, in an amount to be proven at trial.

SIXTH CAUSE OF ACTION

(Breach of Warranty, Express and Implied)

289. Plaintiffs incorporate by reference all of the above allegations as if fully set forth

herein.

290. Uphold promised to consumers on its website, mobile application, promotional materials, and in its blog articles, that it was an industry leader in ensuring account security, that it was PCI DSS compliant, and that it employed numerous safeguards to protect against unauthorized account access.

291. Additionally, it promised that it monitored user accounts for suspicious activity and immediately suspended accounts once suspicious activity occurred, and that it would take immediate action if consumers notified it that their accounts had been breached.

292. This promise and/or description became part of the basis for the bargain by which Plaintiffs and the Class Members used Uphold's services.

293. Uphold did not conform to these promises, in that it employed substandard security measures, inadequate 2FA, and numerous other security lapses as described throughout this Complaint.

294. As a result of this breach of warranty, Plaintiffs' and the Class Members' accounts were breached by cybercriminals.

295. Plaintiff and the Class Members have suffered injury in fact and have lost money and property as a result of Uphold's unlawful and unfair practices, in that, among other things, Uphold's misrepresentations are a material reason that Plaintiffs and the Class Members utilized Uphold's service and paid Uphold's fees.

296. Plaintiffs relied on Uphold's representations about the strength of its security protocols in deciding to use Uphold's cryptocurrency exchange, and Plaintiffs would not have used Uphold's services had Plaintiffs' been aware that Uphold's security protocols were different than those represented.

SEVENTH CAUSE OF ACTION

(Negligent Misrepresentation)

297. Plaintiffs and the Class Members incorporate by reference all of the above allegations as if fully set forth herein.

298. Uphold owed Plaintiffs and the Class Members a duty of care not to misrepresent facts and characteristics of its services.

299. Uphold's representations about its security measures and protocols, as described throughout this Complaint, were false.

300. In making these false representations to Plaintiffs and the Class Members, Uphold failed to exercise due care.

301. These misrepresentations were material, in that Plaintiffs and the Class Members would not have used Uphold's services if they had known that the security measures were inadequate.

302. Justifiably relying on Uphold's misrepresentations, Plaintiffs and the Class Members transacted and stored their currency on Uphold's cryptocurrency exchange, resulting in the loss of their funds when cybercriminals exploited Uphold's inadequate security to breach their accounts.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and all Class Members pray that the Court rule as follows by:

A. Determining that this action is a proper class action pursuant to Rule 23(a) and 23(b)(3) of the Federal Rules of Civil Procedure on behalf of the Class as defined herein, and a certification of Plaintiffs as class representatives pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Awarding all remedies available at law or by equity, including actual, consequential, compensatory, and punitive damages, or disgorgement, in an amount to be determined at trial, against all Defendants, jointly and severally;

C. Awarding pre- and post-judgment interest;

D. Awarding Plaintiffs and Class Members their costs and expenses in this litigation, including reasonable attorneys' fees and experts' fees and other costs and disbursements; and

E. Awarding Plaintiffs and other Class members such other and further relief the Court deems appropriate.

DEMAND FOR TRIAL BY JURY

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury on all issues so triable.

Respectfully Submitted,

KRONENBERGER ROSENFELD, LLP

Dated: February 25, 2022

/s/ Karl S. Kronenberger

Karl S. Kronenberger (NY Bar No. 4631578)
Katherine E. Hollist (*pro hac vice* forthcoming)
150 Post Street, Suite 520
San Francisco, CA 94108
Telephone: (415) 955-1155
Facsimile: (415) 955-1158
karl@KRInternetLaw.com
kate@KRInternetLaw.com

Attorneys for Plaintiffs and the Proposed Class